UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,673	03/30/2001	Taras Malivanchuk	063170.6286	6128

5073 7590 03/17/2006

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,673	MALIVANCHUK ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Taghi T. Arani
Primary Examiner
AU 2131

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-33 are examined and pending.

Claims 25-33 are newly added.

Response to Amendment

2 This Office action is responsive to Applicant's amendment filed 12/05/2005.

Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground (s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim1-2, 5-7, 10-12, 15-17, 20, and 25-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (IDS #5), US Pat. No. 6, 067, 410 (prior art of record) as applied and further in view of US 2002/0178375 to Whittaker et al. (hereinafter "Whittaker").

As per claims 1, 6, 11 and 16, and 21-32 Nachenberg is directed to an emulation repair system (ERS) which restores virus-infected computer files to their uninfected states [see abstract] comprising:

scanning the computer file [system] for the malicious code [Nachenberg teaches scanning the computer system for the malicious (or virus) code and identifying the type of virus, see col. 6, lines 37-40, see also, col. 10, lines 33-54];

identifying the malicious code;

retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer file [system] to a state as the computer file [system] existed prior to modification by the malicious code [Nachenberg teaches a virus definition file (i.e. a data file) comprising an entry or virus definition for each known virus. Each virus definition contains information specific to a virus or a family of such viruses, see col. 7, lines 54-57. That is, the ERS uses the virus type at input as an index to an appropriate virus definition in virus definition file, see col. 7, lines 58-60]; and

executing the at least one command to restore the computer file [system] to the state as the computer file [system] existed prior to modification by the malicious code, wherein the at least one command is used for restoring at least a portion of the computer system [Nachenberg further teaches that the virus definition of the virus definition file includes an index to an associated overlay file appropriate for the virus, see col. 7, lines 61-65], and wherein the information relating to the malicious code further comprises at least one command for curing a file infected with the malicious code, **recited in claims 21-24** [i.e. virus definitions of virus definition file are used for decrypting the virus and for identifying the appropriate one of overlay module, see col. 9, lines 1-16, see also, col. 8, lines 20-31 and that overlay module includes code (i.e. commands) for locating and co-opting virus repair code to restore host file (i.e. executing at least one command to restore (and curing)) the computer system and/or infected file to the state as it existed prior to modification by the malicious code), see col. 10, lines 20-32].

It is noted (as persuasively argued by the Applicant) that Nachenberg is silent to disclose restoring the computer system other than the host file.

Nachenberg fails to disclose executing the at least one command comprises modifying a registry file or stopping a process recited in **claims 25-32.**

However, in an analogous art, Whittaker teaches a protective program (executing commands) for restoring the computer system by a malicious code to the state as the computer system existed prior to modification by the malicious code [paragraph 0016, 0021-0024]. Whittaker further teaches executing the at least one command comprises modifying a registry file [paragraph 0054, paragraphs 0073-0075] or stopping a process [paragraph 0039].

Therefore, it would have been obvious to one of ordinary skill in the art to modify the method/system of Nachenberg, to incorporate the protective program, taught by Whittaker, because detecting malicious code at the application level (host file as is the case in Nachenberg) does not prevent the possibility of malicious code accessing the operating system and its registry file.

As per claims 2, 7, 12 and 17, Nachenberg teaches wherein the step of executing the at least one command includes one of reading, writing, and deleting data [i.e., the overlay module designated in thee virus entry of the virus definition file, is written for a specific virus and includes information for locating the host bytes, and if necessary, the virus repair routine in the virus, wherein the overlay module uses this information in conjunction with some combination of overlay, foundation, and virus repair routines to restore the host bytes to their proper locations in the host file and truncate (i.e. delete) the viral code from the host file, see col. 3, lines 27-50. The teaching of Nachenberg clearly suggests reading, writing and deleting as necessary processes to first locate (i.e. read) the host bytes and restoring the bytes to their proper location (i.e. write) and truncate (i.e. delete) the virus code].

As per claims 5, 10, 15 and 20, Nachenberg teaches wherein the data file comprises a plurality of data files, each data file being provided for a particular type of malicious code, each data file including at least one command that can be used for restoring the computer system to a state that existed prior to modification by the particular type of malicious code [i.e. a virus definition files (i.e. a plurality of data files), wherein a virus Id identifies the specific virus or virus strain that ERS is being called upon to repair. Nachenberg discloses three scenarios representing some of the common strategies employed by various viruses for infecting COM, EXE, and SYS files, see col. 4, line 35 through col. 5, line 35, see also col. 7, line 65 through col. 8, line 33].

4. **Claims 3, 8, 13 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg and Whittaker as applied to claims 1, 6, 11 and 16 above, and further in view of Templeton, US Pat. 6, 401,210, filed Sep. 1998.

Nachenberg as modified fail to teach wherein the step of executing the at least one command includes at least one of renaming and deleting a file.

However, Templeton teaches the step of executing the at least one command includes at least one of renaming and deleting a file presents a method of managing a file infected by at least one computer virus [in one embodiment, Templeton teaches a virus bin comprising a database, controlled access directory, or other data structure holding a plurality of files and information fields related to the files. Templeton teaches that an anti-virus process may be used to continually monitor a system for viruses via a memory-resident program providing real-time protection.

The anti-virus process may be used to scan one or more files in a file structure for a virus and the anti-virus process may prompt the user to select an option to deal with viruses that may

be detected. the options comprise: attempt to clean the file, delete the file, rename the file, or move the file to the virus bin, see col. 3, line 40 through col. 4, line 4].

It would have been obvious to one of ordinary skill in the art to modify the repair system of Nachenberg as modified to that of Templeton to rename and delete infected files, because deleting alone would remove the virus from the computer system, but also destroys the files original content while renaming the infected files would preserve the original content while reducing the probability of the file being accidentally used or transferred, see col. 1, lines 22-56].

5. Claims 4, 9, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg and Whittaker as applied to claims 1, 6, 11 and 16 above, and further in view of FIXHAPPY (a Happy99.worm Removal Tool) announced by AntiVirus Research Center (IDS #5).

Nachenberg as modified fail to teach wherein the malicious code modifies at least one file and said method comprises:

reading from the modified file, a name of a second file; and

modifying the second file.

However, The Happy99.worm Removal Tool teaches reading from the modified file, a name of a second file; and

modifying the second file [that is, restoring WSOCK32.DLL modified to hook the mail-sending and newsgroup article-posting routine. Happy99.worm Removal Tool modifies the Windows system directory by deleting SKA.EXE and SKA.DLL files and by removing windows registry modification].

It would have been obvious to one of ordinary skill in the art to modify Nachenberg's repair system to incorporate the feature taught in Happy99.warm Removal Tool to not only restore the content of infected file (s) (in system directory), but also to modify other file(s) infected (in system registry) to reduce the spread of the worm (virus), especially when a user is online or connected to a network, see the document.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 33 is rejected under 35 U.S.C. 102(e) as being anticipated by Whittaker et al., US 2002/0178375.

As per claim 33, Whittaker et al. teach a method for restoring a computer system modified by malicious code, comprising:

determining whether a computer system has been modified by malicious code [paragraph 0021];

identifying a type of malicious code that has modified the computer system [paragraph 0045];

identifying, based on the type of malicious code, one or more potions of the computer system that have been modified [paragraphs 0081-0091; and

executing at least one command to restore identified portions of the computer system

to one or more states that were associated with the identified portions prior to modification by the malicious code [paragraph 0062-0064, see also paragraph 0094].

Note: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

Prior arts made of record, not relied upon:

US 5,822,517 to Dotan

US 6,263,348 to Kathrow et al.

US 6,535,998 to Cabrera et al.

US 5,657,445 to Pearce

US 5,832,208 to Chen et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Primary Examiner
Art Unit 2131
3/10/2006